ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Θέμα Διπλωματικής Εργασίας

Μελέτη διατάξεων ασφαλείας με Φυσικές Μη κλωνοποιήσιμες Συναρτήσεις
Study of security devices with Physical Unclonable Functions

Επιβλέπων: Δρ. Μηνάς Δασυγένης (mdasyg **(at)** ieee .org**) -http://arch.icte.uowm.gr**

Η αξία των δεδομένων σε υπολογιστικά συστήματα αυξάνεται και τα λειτουργικά συστήματα γίνονται ολοένα πιο ασφαλή. Οι φυσικές επιθέσεις στα υπολογιστικά συστήματα για την υποκλοπή ή τροποποίηση αυτών των δεδομένων γίνονται συνεχώς πιο έντονες. Μια εναλλακτική προσέγγιση, αντί να λύσουμε το πρόβλημα με αλγόριθμο σε επίπεδο λογισμικού, είναι να βασίσουμε τη λύση μας σε ένα νέο φυσικό πρωτόγονο. Οι μέθοδοι φυσικής ασφάλειας για την αποτροπή αυτών των επιθέσεων είναι μία τέτοια λύση.

Οι φυσικές μη κλωνοποιήσιμες συναρτήσεις (Physical Unclonable Functions-PUFs) παρέχουν ένα νέο κρυπτογραφικό πρωτόγονο ικανό να αποθηκεύει τα μυστικά με έναν μη πτητικό, αλλά εξαιρετικά ασφαλές τρόπο. Αυτή η τεχνολογία απαιτεί συνεχή επανεξέταση και βελτίωση, όπως ακριβώς και άλλες ανταγωνιστικές τεχνολογίες χρειάζονται ανασκόπηση για να παραμείνουν στην αιχμή της αγοράς. Μπορούν να εφαρμοστούν, σε ένα μεγάλο πλήθος σύγχρονων εφαρμογών. Τα φυσικά χαρακτηριστικά των στοιχείων αυτών, μπορούν να προσδιορίσουν με μοναδικό τρόπο διατάξεις, ως αποτέλεσμα της λειτουργίας των συναρτήσεων της κατηγορίας αυτής. Το στοιχείο αυτό, δίνει μια ξεχωριστή δυνατότητα στις συναρτήσεις αυτές και επιτρέπει να χρησιμοποιείται η έξοδος τους, ως μοναδικό στοιχείο αναγνώρισης. Η μη δυνατότητα κλωνοποίησης της συμπεριφοράς των PUFs, συντελεί στη χρήση τους ως εργαλεία σε μεθοδολογίες, μηχανισμούς και πρωτόκολλα πιστοποίησης, διατάξεων υλικού.

Σκοπός της εργασίας είναι να μελετηθούν γνωστές φυσικές επιθέσεις, που κυμαίνονται από απλές επιθέσεις που απαιτούν ελάχιστες ικανότητες ή πόρους, ως και σε πολύπλοκες επιθέσεις που απαιτούν εκπαιδευμένους, τεχνικούς ανθρώπους και σημαντικούς πόρους. Επίσης θα μελετηθούν η εφαρμογές των PUFs σε σύγχρονες υλοποιήσεις που απαιτούν αυξημένη ασφάλεια σε επίπεδο υλικού. Η πρόθεση είναι να ταιριάζουν οι μέθοδοι προστασίας με τις μεθόδους επίθεσης όσον αφορά την πολυπλοκότητα και το κόστος. Με αυτόν τον τρόπο μπορεί να παραχθεί οικονομικά αποδοτική προστασία σε ένα ευρύ φάσμα συστημάτων και αναγκών. Η θεματική αυτή περιοχή επικεντρώνεται στη μελέτη των ιδιοτήτων, στις παραμέτρους και στο κόστος υλοποίησης των διαφορετικών PUFs, καθώς και στο πιθανό σχεδιασμό, νέων καινοτόμων αρχιτεκτονικών. Για την ολοκλήρωση της έρευνας, θα γίνει βιβλιογραφική αναζήτηση των γνωστών φυσικών επιθέσεων και των αντίστοιχων αντίμετρων για αυτές. Από την μελέτη αυτή, θα επιλεγεί η καλύτερη λύση και με την χρήση γλώσσας περιγραφής υλικού (VHDL), θα γίνει λειτουργική προσομοίωση σε προγραμματιζόμενο ολοκληρωμένο κύκλωμα γενικής χρήσης (Field Programmable Gate Array – FPGA).

Απαιτήσεις: Ψηφιακή σχεδίαση, Προγραμματισμός VHDL, Αρχιτεκτονική FPGA, Πρωτόκολλά ασφάλειας.

Πλεονεκτήματα: Με την παρούσα διπλωματική εργασία ο φοιτητής θα αποκομίσει καλή γνώση σχεδιασμού ψηφιακών συστημάτων, προγραμματισμού με VHDL και την εμπειρία της υλοποίησης σύγχρονων κρυπτογραφικών εφαρμογών για την προστασία της πληροφορίας σε επίπεδο υλικού. Επίσης θα αποκτήσει γνώσεις στις μεθοδολογίες Σχεδίασης Συστημάτων με τη χρήση Γλώσσας Περιγραφής Υλικού (VHDL) και στην λειτουργική προσομοίωσή τους (π.χ. ModelSim).

Ενδεικτική βιβλιογραφία

1. Armknecht, F., Maes, R., Sadeghi, A., Standaert, F., & Wachsmann, C. (2011). A Formal Foundation for the Security Features of Physical Functions.
2. Katzenbeisser, S., Kocabaş, Ü., Rožić, V., Sadeghi, A. R., Verbauwhede, I., & Wachsmann, C. (2012, September). PUFs: Myth, fact or busted? A security evaluation of physically unclonable

functions (PUFs) cast in silicon. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 283-301). Springer, Berlin, Heidelberg.